Get Connected

Internet Safety – Cyber Security Checklist

Learn Something New — Share with Friends & Family

Having a safe community goes beyond safe streets. When you are protected online, you can enjoy the benefits of the digital society.

Protect your personal information

- ○ Use long and strong passwords – the longer the password, the tougher it is to crack. Use capital and lowercase letters with numbers and symbols to create a more secure password.
- ○ Don't share your account passwords and don't use the same password for different online accounts.
- ○ Put your written password reminders in a safe place and away from your computer.

Keep your computer safe

- ○ Keep your security software updated. At a minimum, your computer should have anti-virus and anti-spyware software.
- ○ Never install software from an untrusted source and watch for unwanted add-ons being installed.
- ○ Be cautious about opening attachments and downloading files from emails, regardless of who sent them. Files can contain viruses that can cause your computer to run poorly and can be used to monitor and control your online activity.
- ○ Back up your files: Copy important files onto a removable storage (CDs/DVDs or flash drives/USB stick) or an external hard drive, and store it in a safe place so you have a backup copy if needed.

Beware of scams

- ○ Beware of email, advertisements, popups, and search results you didn't expect; it may be a scammer trying to trick you into sending them money and personal information. This is called "Phishing" and criminals use the information to commit identity theft.
- ○ Don't enter sensitive information into emails, or click links you are unsure about. Legitimate businesses never ask you to send sensitive information through insecure channels.

Continued on other side

Connect with care

- Look for web addresses with “https://”. The “**s**” at the end stands for “secure” which means the site takes extra measures to keep your information safe.
- Secure your home wireless network with a password and encryption.
- Use your browser’s privacy and security settings, such as pop-up blockers.
- Watch your links:
  - If you have a question about a link on a website, put your mouse over the link *without* clicking. Your browser should show you the actual address of the web page where the link will take you. If everything looks okay, you can then click on the link.
  - Is it the official site? Example:
    - service@paypal.com = good
    - service@paypal.com.clickz.com = bad

Talk with your kids

- Make sure your kids know not to share passwords and personal information and to beware of scams or malware advertised as "free” downloads of music, movies, iPads, and software or games. If it looks too good to be true, it probably is!
- Look for teachable moments — if you hear about a scam or get a phishing message, use it as an example with your kids.

Help your community

- Share cyber safety tips with your friends, family and neighbors.
- File cybercrime reports with the Minneapolis Police Department so that cases in Minneapolis can be addressed and documented. Reports can also be submitted to www.ic3.gov (Internet Crime Complaint Center) and the Federal Trade Commission at www.ftccomplaintassistant.gov

More Resources

- Explore resources at www.onguardonline.org for information on protecting yourself online.
- Check out www.stopthinkconnect.org for additional tips on Internet safety.

City of Minneapolis Information Technology Department
March 2014 www.minneapolismn.gov/it/inclusion
612-673-2026

Minneapolis
City of Lakes